





Information Security Program

Plan of Action and Milestones Guide

May 5, 2004

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Preface

As the Department of Health and Human Services (HHS) Information Security Program evolves, this document will be subject to review and update, which will occur annually or when changes occur that signal the need to revise the *HHS Plan of Action and Milestones (POA&M) Guide*. These changes may include the following:

- changes in roles and responsibilities
- release of new executive, legislative, technical, or Departmental guidance
- identification of changes in governing policies
- changes in vulnerabilities, risks, and threats
- Inspector General findings that stem from a security audit.

The HHS Chief Security Officer (CSO) must approve all revisions to the *HHS POA&M Guide*. Revisions are to be highlighted in the Document Change History table. Each revised guidance document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS POA&M Guide* will be issued, and all affected parties will be informed of the changes made.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number / Paragraph Number	Changes Made By
1.0	06/27/2003	Final Release of Document	NA	NA
2.0	05/03/2004	Content update per OMB Memoranda 03-19 guidance.	Entire Document	HHS OIRM

1. Introduction

The Department of Health and Human Services (HHS) is responsible for implementing and administering an information security program to protect its information resources, in compliance with applicable public laws, federal regulations, and Executive Orders, including the *Federal Information Security Management Act of 2002* (FISMA); the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000; and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). To meet these requirements, the Department has instituted the *HHS Information Security Program Policy* document and accompanying *HHS Information Security Program Handbook* document.

The *HHS Plan of Action and Milestones (POA&M) Guide* provides guidance for HHS management and Operating Division (OPDIV) personnel responsible for the appropriate completion and maturity of the POA&M process. The *HHS POA&M Guide* is a reference that provides explanations and assistance to maximize efficiency, reduce vulnerabilities, and streamline the POA&M process.

1.1 Purpose

The *HHS POA&M Guide* provides HHS and OPDIV information security management and system owners with the necessary guidance and procedures for developing, maintaining, and reporting their POA&M. This guide outlines steps to implement POA&M as defined by OMB Memoranda 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly Information Technology (IT) Security Reporting.*

1.2 Background

This POA&M guide incorporates new aspects of the POA&M process prescribed by OMB. Information is included to account for the emphasis that has been placed on formalizing the weakness mitigation process and ensuring weaknesses are appropriately prioritized for mitigation. This guide is created to continue the evolution of the POA&M process into a mature set of activities that results in effective weakness correction.

1.3 Scope

This document applies to all HHS and OPDIV information security leadership, managers, and staff. Any personnel tasked with completing POA&M activities should read this document to become familiar with the POA&M process.

1.4 Document Organization

The remainder of this guide is structured as follows:

- Section 2 highlights the POA&M process, as well as specific Departmental roles and responsibilities.
- Section 3 outlines methods for weakness identification, methods of weakness prioritization, the recommended method for integrating capital planning with the POA&M process, and HHS-approved POA&M reporting requirements.
- Section 4 provides the specific details and formatting requirements for the POA&M report.
- Section 5 summarizes the POA&M process and the benefits of compiling an accurate POA&M.
- Section 6 provides a conclusion summarizing the points of this guide.

Additionally, this guide contains the following appendices:

- Appendix A provides a feedback form to submit comments on the document.
- Appendix B lists the references used in this document.
- Appendix C lists the acronyms used throughout the document.
- Appendix D defines terms most frequently used in this document.
- Appendix E describes Weakness Prioritization Methodologies.
- Appendix F provides a sample POA&M submission.

2. POA&M Overview

A POA&M, also referred to as a corrective action plan, is a management tool that outlines identified information security program and system weaknesses along with the tasks necessary to mitigate them. To facilitate the remediation of weaknesses, the POA&M process provides a means of planning and monitoring corrective actions; defines roles and responsibilities for solving problems; assists in identifying security funding requirements; tracks and prioritizes resources; and informs decision-makers.

2.1 POA&M Definition and Purpose

The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in *programs* and *systems*.[1] HHS and OPDIVs should use POA&Ms to close their security performance gaps, assist the Inspector General (IG) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities.

The POA&M presents the opportunity for the Department to highlight its progress and demonstrate improvements in the quality and security of its information security program. It is also designed to serve as a management tool specific to HHS processes and as a point of comparison for OMB in its assessment of the overall maturity of the federal government's IT security status.

Though the POA&M is considered a comprehensive plan, OMB operates under the assumption that additional, more detailed project management plans exist for each corrective action item identified in the POA&M, and that additional sources (e.g., IG audit reports and risk assessments) are readily available to provide original documentation of each weakness. Thus, each POA&M element should be clearly traceable back to its original source(s).

2.1.1 Importance of the POA&M

Effective remediation of security weaknesses is essential to achieving a mature and sound information security program. As a result, correct implementation and use of the POA&M process are critical elements used to assess information security program implementation by OMB, Congress, and the Office of Inspector General (OIG).

2.1.1.1 System Funding

POA&Ms are used by OMB to assess the state of the federal government's IT security and to aid in OMB's oversight of the federal government and its IT investments. OMB requires tying the POA&M to the budgeting process to evaluate the soundness of an investment. Systems that do not adequately address a plan for securing funding for mitigation of IT security weaknesses can be placed 'at risk' and lose funding. For

[1] OMB Memorandum 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003.

major investments, OMB requires related POA&Ms to be cross-referenced through answers to questions when completing section II.B. of an exhibit 300. The response to all questions in this section of the exhibit 300 should align with weaknesses reported in the POA&M. Answers to question II.B.1(A) in the exhibit 300 ("What is the total dollar amount allocated to IT security for this investment? Please indicate whether an increase in IT security funding is requested to remedy IT security weaknesses, specifying the amount and a general description of the weakness.") should link to the POA&M in the following manner:[2]

- Although the total dollar amount allocated to IT security will not match the POA&M exactly, it will include figures from the POA&M in addition to ongoing security costs.
- The increase in funding necessary to mitigate the weakness should match those listed in the 'Resources Required' column of the POA&M.
- Identification of the security weaknesses noted in the capital planning document should match those identified in the POA&M.

System-level POA&Ms are linked directly to the system budget request through the IT business case, as required in OMB budget guidance, Circular A-11, *Preparation, Submission and Execution of the Budget*. Specifically, the unique project identifier must be reflected on the POA&M for each system POA&M that is part of a capital asset plan and justification (exhibit 300). This identifier will provide the link to agency budget materials. For systems that are covered by an exhibit 53 versus an exhibit 300, the coverage of costs should be denoted as included in an exhibit 53. This effort links the security costs for a system with the security management and performance of a system.

2.1.1.2 Evaluation of the IT Security Program

Congress uses the IG evaluation of an agency's POA&M process in determining the Congressional Security Report Card. In fulfilling its oversight role, it is necessary for Congress to obtain information about an agency's information security activities and FISMA compliance. Therefore, agencies may release to Congress, as requested, the following information from their POA&Ms: (1) type of weakness; (2) key milestones; (3) any milestone changes; (4) source of identification of the weakness; and (5) the status of the weakness.

In addition, having a sound POA&M process is essential to achieving a high score on the President's Management Agenda (PMA). The PMA is a strategy for improving the management and performance of the federal government. Table 1 illustrates that having an effective POA&M process is key to achieving positive results for the IT security component of the E-Government Scorecard.

[2] Refer to the *HHS IT Security Capital Planning Guide* for further guidance on this topic.

Table 1. Capabilities Needed for the President's E-Government Scorecard

Status	Capabilities
Green	▸ Demonstrate consistent progress in remediation of IT security weaknesses through their POA&Ms ▸ Have IG verify that there is a Department-wide IT security POA&M process ▸ Have 90% of operational IT systems properly secured (e.g., certified and accredited), including mission-critical systems.
Yellow	▸ Demonstrate consistent progress in remediation of IT security weaknesses through their POA&M updates and either: – Have IG verify that there is a Department-wide IT security POA&M process – Have 80% of operational IT systems properly secured (e.g., certified and accredited).

2.2 Benefits of the POA&M

Through the process of strategically addressing vulnerabilities in the POA&M, the missions of HHS and the OPDIVs can proceed without interruption or failure in appropriate service delivery. Beyond its function as the primary authoritative IT security management tool, the POA&M has other benefits related to producing valuable trending and analysis, supporting IT business cases, maintaining institutional knowledge, and facilitating effective communication. Each of these uses provides HHS and OPDIVs with tighter control over their IT security program and increases the efficiency of IT security management.

- **Producing Trending and Analysis.** The POA&M can be used as a historical data source for management reporting and business intelligence on the costs, effort, and time to mitigate IT security weaknesses. The type of weaknesses occurring can be tracked, as well as the rate of recurrence. The POA&M provides the ability to conduct analyses by system, program, OPDIV, or across HHS as a whole.
- **Supporting Business Cases.** A comprehensive POA&M, with accurate and reliable financial estimates, provides traceability and justification for additional security funds to mitigate weaknesses.
- **Maintaining Institutional Knowledge.** A mature POA&M prevents reliance on one individual to retain and communicate information pertinent to a system or an entire program.
- **Facilitating Effective Communication.** The POA&M facilities communication and coordination among personnel, such as the OPDIV Chief Information Officer (CIO), OPDIV Information System Security Officer (ISSO), budget personnel, and program officials.

2.3 Roles and Responsibilities

Both within HHS and across the federal government, many roles now include POA&M responsibilities. POA&Ms are designed to be used predominately by Departmental CIOs, CSO, program officials, ISSOs, agency IG, and system owners to track the progress of IT weakness corrective actions.

OMB's guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems that they operate and control (e.g., for program officials this includes all systems that support their operations and assets). The HHS CIO delegates to the HHS CSO the oversight and maintenance of the Department POA&M process. For OPDIVs, the overall responsibility rests with the CIO and the senior information security official (e.g., CSO, ISSO). While much of the focus of security at an OPDIV involves IT security professionals, collaboration should occur with OPDIV senior management to ensure weakness mitigation plans are in alignment with the OPDIV's mission and that funding is allocated appropriately. Coordination with budget personnel ensures weakness mitigation funding is incorporated into capital planning where necessary.

The following POA&M roles and responsibilities outlined in this guide are in addition to those designated in the *HHS Information Security Program Policy*.

2.3.1 Department Level

At the HHS Department level, the POA&M aids in the oversight of security issues. The following department leadership roles have specific responsibilities related to the POA&M process:

- HHS CIO
- HHS CSO
- IG.

2.3.1.1 HHS CIO

- assigns responsibility to the HHS CSO for oversight and management of the Department POA&M
- is responsible for the transmission of agency progress in correcting weaknesses reflected in the POA&M and the results of independent IG inspections to the OMB Director
- reports to OMB the results of HHS system and program reviews and progress in implementing the POA&M.

2.3.1.2 HHS CSO

- oversees and maintains the department-wide security program POA&M
- works with the IG to ensure the development and maintenance of a comprehensive POA&M program
- coordinates and analyzes the POA&M process for improvements
- ensures the POA&M is used to assess Department-wide security weaknesses
- allocates proper resources to permit identification and remediation of Office of the Information Resource Management (OIRM) program and system weaknesses.

2.3.1.3 IG

- works with the HHS CSO, OPDIV program officials, and system owners to conduct independent verification and validation of the POA&M process
- reports the findings of the independent verification and validation on POA&M implementation.

2.3.2 OPDIV Level

At the OPDIV level, the POA&M aids in the identification and evaluation of security issues among individual OPDIVs. The following types of OPDIV-level roles and responsibilities related to the POA&M process should exist (varying titles and distribution of responsibilities may exist within an OPDIV):

- OPDIV Heads/Management Officials
- OPDIV CIOs
- OPDIV CSOs
- OPDIV ISSOs
- System owners.

2.3.2.1 OPDIV Heads/Management Officials

- ensure IT security management decisions reduce risk to an acceptable level
- work with OPDIV CIOs to ensure funding is available for weakness mitigation.

2.3.2.2 OPDIV CIOs

- allocate proper resources to permit identification and remediation of weaknesses
- oversee and monitor progress of the OPDIV POA&M implementation and remediation efforts.

2.3.2.3 OPDIV CSOs

- create and manage OPDIV IT security program POA&M
- track and maintain all POA&M activities on at least a quarterly basis
- ensure provision of the OPDIV's quarterly update to the HHS CSO according to the defined reporting schedule
- monitor progress of the OPDIV POA&M implementation and remediation efforts
- inform management of weakness mitigation progress
- work with OPDIV ISSOs and system owners to reduce risk
- ensure system POA&Ms are developed and maintained by personnel
- ensure all POA&M data reflects the current state of security weaknesses across the OPDIV and is consistent with related federal and Departmental reporting
- submit the OPDIV POA&M report (program and system POA&Ms) to the HHS CSO quarterly, according to the defined reporting schedule.

2.3.2.4 OPDIV ISSOs

- work with system owners to develop, implement, and manage corrective action plans for all systems they own and operate
- ensure that OPDIV POA&Ms contain appropriate details, as required by OMB and the Department
- centralize OPDIV POA&M information
- conduct follow-up to verify corrective action's status
- update OPDIV CSO, on regular basis, the progress of the mitigation activities of each weakness.

2.3.2.5 System Owners

- work with OPDIV ISSOs to develop, implement, and manage system-level corrective action plans for all systems that support their operations and assets
- update OPDIV management regularly (at the direction of the OPDIV CIO) on the progress of weakness remediation efforts, enabling the OPDIV CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

3. Weakness Remediation Process

Weakness remediation consists of a cycle that entails the following steps depicted in figure 1.

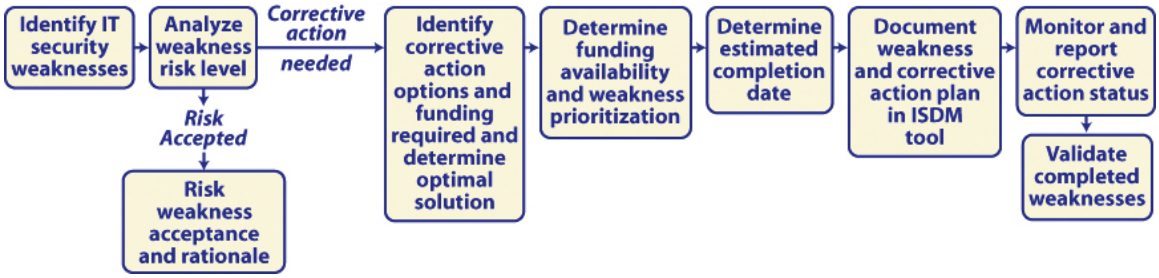

Figure 1. The POA&M Process for Weakness Remediation

The following section of this guide describes the methodology to be applied for implementing the steps in this process.

3.1 Identifying Weaknesses

Weaknesses to be recorded and tracked throughout the POA&M can be identified by either a reactive or proactive means. Reactive weakness determination indicates that outside auditors or reviewers identified the weakness. Proactive weakness determination occurs by conducting regular program and system reviews using self-assessments.[3]

Sources of weaknesses can include the findings from reviews such as:

- IG audits
- General Accounting Office (GAO) audits
- Chief Financial Officer (CFO) audits
- National Institute of Standards and Technology (NIST) Self-Assessments — any NIST self-assessment result less than level 3 (for controls that are required for a system) is considered a weakness.
- risk assessments
- penetration tests.

3.1.1 Including Weaknesses

POA&Ms must include *all*[4] security weaknesses, not just material weaknesses, associated with HHS and OPDIV IT security systems and programs. The POA&M is the authoritative department-wide management tool, and as such, it should represent an all-inclusive view of identified security weaknesses. To ensure

[3] Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.
[4] Meaning all weaknesses identified that require a corrective action.

comprehensiveness, a separate POA&M must be developed for every program and system for which weaknesses were identified. The two types of weaknesses—program and system—are described in further detail below.

- **Program Weaknesses.** A program weakness impacts multiple IT systems as a result of a deficiency in the IT security program. Program weaknesses are addressed separately from individual system weaknesses. An example of a program weakness is: *Security policy is not updated with latest legislative guidance*.
- **System Weaknesses.** A system weakness pertains to the management, operational, or technical controls of a specific IT system. Each set of system-specific weaknesses is noted under separate headers in a POA&M. An example of a system weakness is: *System has not been certified and accredited/authorized to operate*.

3.1.2 Risk-Based Exceptions

In some cases, a specific corrective action plan may not exist for a weakness because the weakness is considered an acceptable risk (OPDIV management should sign-off that the risk is acceptable). As such, the weakness is not required to be included in the POA&M. A record of the risk acceptance must be documented since risks can change over time. OPDIVs should record their rationale for accepting the risk. The weakness should be reviewed periodically for changes in the acceptable risk level.

3.2 Determining Corrective Action Plan Options

There are often multiple methods of mitigating a weakness. Methods should be analyzed for appropriateness in resolving the weakness fully and viewed for long-term implications. At this time, the cost for each corrective action plan option must be estimated and analyzed to determine short-term and long-term solution capabilities.

3.3 Determining Funding Availability

Resources for weakness remediation can be obtained through the following means:

- using current resources marked for security management of the system or program
- reallocating existing funds or personnel
- requesting additional funding.

If new funding is required, it is imperative to ensure the capital planning process is correctly utilized to gain the necessary funds. Integrating IT security costs with the capital planning process ensures that security is included in the agency's enterprise architecture, supports business operations, and is funded within each information system over its life cycle. Funding requests for all associated system security costs

occur through the creation of an exhibit 300 (for major systems) or 53 (for all other systems).

3.4 Prioritizing Weaknesses

FY03 FISMA guidance requires federal agencies to prioritize weaknesses within POA&Ms to help ensure that significant IT security weaknesses within POA&Ms take precedence and are immediately mitigated. Additionally, FISMA also charges the agency IG with determining if POA&M weaknesses are adequately prioritized.

In addition to FISMA requirements, two other factors drive the need for POA&M weakness prioritization:

- **Resource Limitations.** Often, agencies cannot obtain the funding and personnel resources necessary to mitigate every weakness identified in the POA&M. Therefore, by prioritizing weaknesses, agencies can ensure that high-priority weaknesses receive immediate funding and personnel resources to mitigate risks.
- **Varying Risk Levels.** Not all weaknesses identified in program and system POA&Ms carry the same risk level. With the reality of resource limitations, it is essential that high-risk weaknesses receive timely attention.

The key to effective prioritization is rank ordering corrective actions to address weaknesses according to specific criteria. The rank-ordering criteria enable HHS and OPDIVs to prioritize corrective actions quantitatively against factors that are specific to their operating environments. Examples of prioritization criteria can include:

- risk level of weakness and risk level of system
- department security themes
- specific security control implementation
- cost effectiveness of implementing the corrective action
- length of time since the weakness was identified.

3.4.1 Basic Weakness Prioritization

In its simplest form, basic weakness prioritization focuses on two essential prioritization criteria: system categorization and weakness risk level.

System categorization should be determined in the system's risk assessment according to the criteria articulated in the Federal Information Processing Standards (FIPS) Publication 199, *Security Categorization of Federal Information and Information Systems*. According to FIPS 199, systems' categorization should be classified as high, moderate, or low, according to confidentiality, integrity, and availability criteria.

The second criterion for basic weakness prioritization is the potential impact of the weakness if it is unresolved. The identified weakness' potential impact is listed in the

POA&M as high, medium, or low. Appendix E contains examples of how this prioritization strategy is conducted.

3.4.2 Compound Weakness Prioritization

An example of a more detailed corrective action prioritization methodology was created from several components of the forthcoming NIST SP 800-65, *Integrating IT Security Into the Capital Planning and Investment Control Process* guidance document. NIST developed this methodology as a means of prioritizing POA&M weaknesses via an approach that rank orders POA&M corrective actions according to the Federal government security priorities, the agency's missions and goals, total corrective action cost to mitigate all weaknesses, and IT security improvement criteria.

The NIST methodology can be challenging to implement immediately, as it is a detailed methodology. As a result, a phased approach may be desired that builds upon successive steps in the prioritization process. Appendix E contains specific examples of how this prioritization strategy is conducted.

3.5 Determining an Estimated Completion Date

The estimated date of completion for each weakness should be determined based on realistic timelines for resources to be obtained and associated steps to be completed. Although it may take 30 days to complete specific weaknesses individually, it may not be possible to complete all these weaknesses during the same time period if using the same staffing resources. The completion date should be based on the outcome of prioritization decisions and resource availability.

3.6 Documenting the Corrective Action Plan

OMB established the foundational structure of the POA&M to provide consistency in the presentation of information. This structure improves the ability to use the POA&M to locate information and organize details for analysis.

3.7 Monitoring and Reporting POA&M Activity

POA&M maintenance and reporting demonstrates continuous progress toward an improved IT security program. The POA&M should be managed through oversight and updating information as the status of weakness mitigation process changes.

The information in the POA&M should be maintained continuously and a quarterly status report must be provided to communicate overall progress in identifying and mitigating weaknesses. The format of the quarterly POA&M status report is shown in table 2.

Table 2. Format of Quarterly Update to OMB

Quarterly POA&M Updated Information	Programs	Systems
Total number of weaknesses identified at the start of the quarter		
Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter		
Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled		
Number of weaknesses for which corrective action has been delayed, including a brief explanation for the delay		
Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.)		

Each OPDIV is expected to update their POA&Ms and POA&M summary reports continuously and be prepared to submit them at the request of the HHS CSO, which may be seven to fourteen business days in advance of the OMB quarterly deadlines. The Department will collect each OPDIV POA&M and submit one compiled HHS POA&M to OMB.

3.8 Validating Weakness Completion

FISMA guidance directs that the 'Completed' status for a weakness should be used only when a weakness has been fully resolved and the corrective action has been tested. Therefore, it is imperative to incorporate corrective action testing into the weakness mitigation process.

4. POA&M Components and Formatting

Each POA&M submission is organized across 11 columns that contain information about the weakness and associated remediation activities. This section of the guide describes in detail the contents and formatting of each of the 11 columns, inclusive of OMB and HHS requirements, for reporting each weakness. The POA&M columns are highlighted in table 3 and detailed in the following subsections. For samples of a completed program and system POA&M, see appendix G.

Table 3. POA&M Column Descriptions

Column	Heading	Contents—How to Complete
1	Weakness Identifier	The weakness identifier will be used to track and correlate weeknesses that are ongoing throughout quarterly submissions within the Department.
2	Weaknesses	A weakness represents any program or system-level information security vulnerability that poses an unacceptable risk of compromising confidentiality, integrity, or availability of information.
3	Point of Contact (POC)	A POC is the organization or title of the position within the Department that is responsible for the weakness' mitigation.
4	Resources Required	Resources required include the funding or man-hours necessary for mitigating a weakness. The type of funding (current, new, or reallocated) should be noted.
5	Scheduled Completion Date	Completion dates should be set based on a realistic estimate of amount of time it will take to collect the resources for the corrective action and implement/test the corrective action.
6	Milestones with Completion Dates	Milestones with completion dates outline the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step.
7	Changes to Milestones	Changes to milestones indicate the new estimated future date of a milestone's completion if the original date is not met.
8	Identified in CFO Audit or other review?	This column indicates the review type, reviewing organization, and date that identified the weakness.
9	Status	The status indicates the stage or state of the weakness in the corrective process cycle (Completed, Ongoing, or Delayed).
10	Comments	The comments column is used for additional detail or clarifications and must be used if there is a delay.
11	Risk Level	The risk level is a ranking that determines the impact of a vulnerability to the system, data, and/or program.

*Once an agency has completed the initial POA&M, no changes should be made to the data in columns 1, 2, 5, 6, and 8.

4.1 Weakness Identifier

Each weakness on the POA&M should be assigned a weakness identifier[5]. The weakness identifier will be used to track and correlate weaknesses that are ongoing throughout quarterly submissions within the Department. The numbering schema used to generate the weakness identifier for a system consists of a combination of the name of the associated system, the quarter the weakness is first recorded on the POA&M, the fiscal year the weakness is first recorded on the POA&M, and a sequence number (e.g., System Name_Quarter_Fiscal Year_Weakness Number). Note: A program weaknesses identifier uses the term 'Program Name' in lieu of a system name at the beginning. See figure 2 for a sample system weakness identifier.

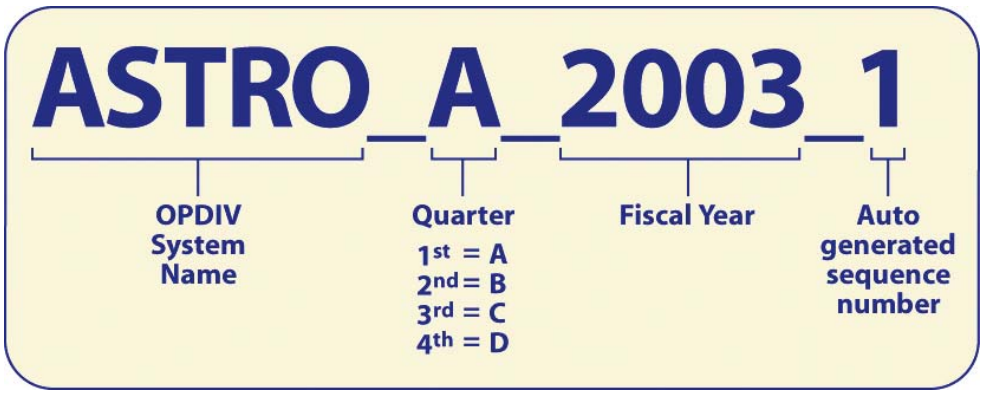

Figure 2. Sample System Weakness Identifier

In the sample above, 'ASTRO' is the OPDIV's system name or acronym. This acronym becomes important for sorting POA&Ms by system at both the OPDIV and Departmental levels. The letter 'A' represents the quarter in which the weakness was first identified and entered onto the POA&M. The number '2003' represents the fiscal year in which the weakness was identified and submitted. The value '1' represents the place in numerical order in which this particular weakness was entered on the POA&M for the ASTRO system. In this case, this weakness identifier indicates this is the first weakness that has been entered in this submission.

4.2 Weakness Description

In POA&M terminology, the term 'weakness' refers to any program or system-level information security vulnerability that poses an unacceptable risk of compromising confidentiality, integrity, or availability of information. A program or system weakness represents the gap between current program or system status and the IT security program's intended long-term goals.

When reporting weaknesses, consideration must be given to the level of detail revealed in the POA&M. Detailed descriptions are *not* necessary, but sufficient data is required to permit oversight and tracking. POA&M authors must remain continuously

[5] While a required column for each weakness, the weakness identifier is not counted by OMB as one of the 11 columns on the POA&M entry.

aware that sensitive information should not be revealed in the description of the weakness or associated milestones. If sensitive information were to be obtained by a person not permitted to access the system or someone outside the organization, the system may be exposed to unnecessary risk. To the extent possible, POA&M authors should use the type of language commonly found in GAO and IG reports, such as "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not performed prior to system access," "physical access controls are insufficient," etc. Where it is necessary to provide more detailed data, the POA&M should explicitly note the special sensitivity in the 'Comments' column.

Table 4 contains examples of weaknesses that contain improper sensitive information and how these statements can be acceptably reworded.

Table 4. Unacceptable vs. Acceptable Wording of Weaknesses

Less Appropriate	Reason Improvement Needed	More Appropriate
Passwords are easily guessed	Sensitivity level	System does not adhere to password policy
Telnet port open, allowing access by outside users	Sensitivity level	Unnecessary services are enabled
Penetration test to be conducted	This is a milestone that will mediate a weakness	Security reviews are not adequate to determine weaknesses
Additional operational controls needed	Too vague	All required background investigations not completed

Although it is important not to provide information that could directly jeopardize the security of the system, enough information must be provided to demonstrate that there is specific awareness of the weakness and that specific actions are taking place to address the weakness.

Useful Tips:

- Ensure a weakness does not identify specific system or program specific sensitive information that would compromise the integrity, availability, and confidentiality of the data.
- Ensure a weakness is described appropriately and not listed as a corrective action. For example,

    - incorrect 'Weakness' description: *Draft system security documentation*
    - correct 'Weakness' description: *System does not have up-to-date system security plan.*

4.3 Point of Contact

For each weakness identified, a point of contact (POC) must be listed on the POA&M. The POC is the position/role (e.g. ISSO, ASTRO system owner) that will be responsible for resolving the weakness. Using specific names on the POA&M is not acceptable as personnel may leave and/or responsibilities may change. It is not adequate to simply reference the specific OPDIV name as the POC. The organization/office within the OPDIV responsible for correcting the weakness should be apparent.

Useful Tips:

- Ensure that the POC is identified as a designated position/role within an OPDIV.
    - Do not identify solely the OPDIV name; rather include position/role and if appropriate, the specific office within that OPDIV.
    - Do not list personnel names and phone numbers for the POC.
- Ensure that a POC is listed for all weaknesses.

4.4 Resources Required

Every weakness requires resources, staff, and/or funding to be corrected. The type and amount of resources required for corrective actions will vary. If existing government personnel in the OPDIV will correct the weakness and no new funding is required, the POA&M should identify the amount of time it will take to complete the corrective action (e.g., 60 hours) and that it is performed by current staff. The resources required must be based on the total amount of resources needed to fulfill all the milestones for weakness correction. The type of funding (current, new, or reallocated) should be noted with the dollar and/or manpower in this section.

Useful Tips:

- Ensure that all weaknesses have resources identified to mitigate the vulnerabilities.
- Ensure that resources are identified as man-hours or monetary values. For example,
    - incorrect ‘Resources Required’ description: *From Existing Resources*
    - correct ‘Resources Required’ description: *$75,000, current funding or 120 hours, new staff.*
- Ensure that monetary funding is identified as “current resources”, “new resources”, or “resources reallocated from existing funding” (also suggested to include if new staff is required or existing staff will be utilized when listing man hours).

4.5 Scheduled Completion Date

The scheduled completion date should be determined based on a realistic estimate of the amount of time it will take to collect the resources for the corrective action and complete the corrective action. Draft documents do not receive credit for completion by OMB and Congress, so it is important to factor interagency review into the timeline.

This column should be formatted to include the month, day, and year of estimated completion. Once the scheduled completion date is entered on the POA&M, it should not be changed. Progress toward completion is tracked through milestones. If the time to correct the weakness extends beyond the scheduled completion date, the status of the weakness should be changed to 'delayed' and reasons for the delay should be noted in the 'Comments' column.

Useful Tips:

- Ensure that all weaknesses have a scheduled completion date. For example,
    - incorrect 'Scheduled Completion Date' description: *2 years*
    - correct 'Scheduled Completion Date' description: *10/31/2004.*
- Ensure that the initial scheduled completion date is not changed if the weakness is mitigated prior to or after the original date.

4.6 Milestones with Completion Dates

Each weakness will have one or more milestones associated with it. The key milestones associated with each corrective action are the items that should be identified in this column on the POA&M. The number of milestones articulated per weakness should reflect the number of steps or corrective actions necessary to address the weakness.

Including anticipated completion dates with each milestone facilitates tracking progress toward weakness mitigation. Each milestone within the POA&M should include an anticipated date of completion, and the date shall be formatted to list the month, day, and year. Once milestones and completion dates are entered in this column, changes should *not* be made. If estimated milestone completion dates change, the new expected date should be recorded in the 'Changes to Milestones' column and reasons for the change should be noted in the 'Comments' column.

Milestones should effectively communicate the major steps that will be performed to mitigate a weakness. Milestones should not simply re-state that the weakness will be completed by repeating the weakness description. For example, appropriate milestones for a weakness like, "Identification and authentication processes need to be more stringent" would read:

- evaluate methods for strengthening identification and authentication
- develop procedures to standardize accepted authentication process
- implement appropriate authentication process.

Useful Tips:

- Ensure that a milestone is described appropriately and listed for all weaknesses.
    - The milestone should be detailed as a specific requirement to correct an identified weakness.
- Ensure that all milestones are numbered.
    - If there is more than one milestone for a weakness, list and number the milestones in the order they should be executed.
- Ensure that each milestone has an anticipated completion date.

4.7 Changes to Milestones

If a situation exists, that prevents a milestone and/or overall corrective action from being completed on time, the new estimated date of completion should be identified in the 'Changes to Milestones' column. No changes should be made to the original estimate in either the 'Scheduled Completion Date' or the 'Milestones with Completion Date' columns. The date should be formatted to include the month, day, and year of estimated completion. The reason for the change in milestone completion should be recorded in the 'Comments' column (see section 4.10).

Useful Tips:

- Ensure that a change to a milestone has been accurately identified in this column.
    - Update the date to include the new proposed date.
- Do not change the original date listed in the 'Milestones with Completion Date' column.

4.8 Identified in CFO audit or other review?

This column should be used to list the method by which the weakness was identified. Section 3.1 outlines the most common sources and methods of identifying POA&M weaknesses. When recording the source that identified the weakness, ensure that the information includes the type of review (e.g., IG audit, self-assessment, IG FISMA review) and the date (month and year). In the event that multiple sources cite a specific weakness, list the additional sources and dates in the 'Comments'

column. The organization that conducted the review should be clearly stated (OPDIV, IG, etc.).

Useful Tips:

- Ensure that all weaknesses have corresponding sources identified.
- Ensure the date (month and year), review type, and reviewer is communicated. For example,
    - *IG Audit, September 2003*
    - *NIST Self Assessment, December 2003 (system owner)*.

4.9 Status

All corrective actions should have an assigned status. The status of a corrective action can be designated as: 'Completed', 'Ongoing', or 'Delayed'. The Completed status should be used only when a weakness has been fully resolved and the corrective action has been tested. When listing items as 'Completed' also include the date of completion in this column. Maintaining the POA&M to indicate the current status of a corrective action helps to demonstrate the POA&M is being used as a management tool and is part of an ongoing process.

Useful Tips:

- Ensure that all weaknesses have a status identified.
    - Status should be selected as 'Completed,' 'Ongoing,' or 'Delayed.'
    - Status should be accurately reflected based on the scheduled completion date.
    - Status refers to the status of the entire weakness; this area is not used to denote the status of individual milestones.

4.10 Comments

The 'Comments' column provides a space where additional detail or clarification for the POA&M weakness may be entered. This column is used to explain additional steps taken to remedy weaknesses and reasons why delays are occurring. The 'Comments' column should identify other, nonfunding, obstacles, and challenges to resolving the weakness (e.g., lack of personnel or expertise or developing new system to replace insecure legacy system). Also, if the same weakness is found repeatedly in subsequent reviews, list the additional sources and dates of finding in the 'Comments' column. This method provides the Department with a means of more accurately conveying to the IG, OMB, or any other external stakeholder what is occurring with a specific weakness.

Useful Tips:

- The 'Comments' column should be used when:
  - additional explanations can provide insight into the challenges being faced and likely dependencies that can impact the weakness mitigation
  - scheduled completion date has not been met; any weakness that has been listed as 'Delayed' should be addressed to provide further clarification or reason for delay.

4.11 Risk Level

The 'Risk Level'[6] column has been added to the POA&M tool to denote the determined potential impact of a weakness on the system, data, and/or program. The exploitation of weaknesses can result in loss or degradation of the integrity, availability, and confidentiality of a system. Some tangible impacts can include loss of confidential or proprietary data, repairing the system or data, loss in revenue, damage to an organization's credibility due to misinformed data to the public, or the level of effort and manpower required to correct problems caused by an exploited weakness. An appropriate risk level should be assigned to each weakness based on the potential impact and threat likelihood of exploitation of the weakness.[7] Risk level definitions can be designated as high, medium, or low.

4.11.1 Risk Level Determination

The risk level determination process[8] encompasses the following steps:

- Step 1–Determine the likelihood of the identified system threat exploiting a specific identified vulnerability.
- Step 2–Determine the impact to a system's operation and information should a threat exploit the specific identified vulnerability.
- Step 3–Determine the overall risk for the specific identified vulnerability.

The equation shown in figure 3 summarizes how risk is determined for each observation:

Figure 3. Risk Score

[6] While a required column for each weakness, the weakness identifier is not counted by OMB as one of the 11 columns on the POA&M entry.

[7] Draft NIST SP 800-30, Revision A, *Risk Management Guide for Information Technology System*, January 2004.

[8] Process based on Draft NIST SP 800-30, Revision A, *Risk Management Guide for Information Technology Systems*, January 2004.

4.11.1.1 Step 1–Determine the Likelihood

Likelihood is determined by considering the intersection of threats and vulnerabilities. The likelihood that a vulnerability will be exploited by a threat will be assessed and described as high, medium, or low. Factors that govern the likelihood of threat exploitation include threat capability, frequency of threat occurrence, and effectiveness of current countermeasures. The descriptions shown in table 5 are used to determine the likelihood level for a threat/vulnerability pair.

Table 5. Likelihood Levels

Likelihood Levels	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

4.11.1.2 Step 2–Determine the Impact

Impact refers to the magnitude of potential harm that may be caused by threat exploitation. Impact is determined by the value of the resource at risk, both in terms of its inherent (replacement) value and its importance (criticality) to organization's mission. The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. Table 6 provides a description for each level of impact.

Table 6. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Medium	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

4.11.1.3 Step 3–Determine the Risk

After evaluating likelihood and impact, the assessment team will use a risk level matrix with the ratings of high, medium, and low to determine the degree or level of risk to which a system, facility, or procedure might be exposed if a vulnerability is exploited. The level of risk equals the intersection of the likelihood and impact values. For example, based on figure 4, if the likelihood level is 'high' and the impact level is 'low' for a threat/vulnerability pair, then the risk level would be 'medium.'

	Impact		
Threat Likelihood	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Figure 4. Risk Level Matrix

5. Formalizing the POA&M Process

A process is a series of actions implemented to produce a desired result. A mature process formalizes these actions. A comprehensive POA&M process includes the necessary steps to form a repeatable cycle that effectively corrects weaknesses.

The POA&M process should include:

- formal process development
- identification of inputs to the POA&M process
- POA&M documentation development and reporting
- weakness remediation
- information verification
- post remediation improvement efforts.

5.1 Formal Process Development

In creating a comprehensive process, documenting policy and procedures related to the POA&M allows a consistent approach to be outlined and used for accountability. It is also important to assign specific roles and responsibilities to personnel, and ensure adequate training is in place to aid personnel in understanding and carrying out assigned roles and responsibilities. To ensure weaknesses are corrected according to standards, prioritization criteria should be identified and a process for budget decisions to ensure the appropriate use of funding should be developed.

5.2 Identifying Inputs to the POA&M Process

Identification of inputs to the POA&M process is an integral part of the formalization process. An organization should take time to review all the sources related to the POA&M process (e.g., internal and external audits or self assessments). An organization should also evaluate weaknesses for risk acceptability and ensure discussions take place on a regular basis with management regarding risk-based decisions. It is also important to ensure a corrective action plan is created for all weaknesses that require remediation.

5.3 POA&M Documentation Development and Reporting

POA&M documentation development and reporting is another important component to formalizing the POA&M process. All weaknesses requiring corrective action should be included in the POA&M documentation. The POA&M documentation should be created according to the standards and recommendations set forth by OMB and HHS. In addition, it is imperative that reporting guidelines are followed.

5.4 Weakness Remediation

The rate of weakness remediation is an output that signals success in the process. If an organization's POA&M process is mature, it will make evident the efficacy of corrective actions and ensure that the organization's weaknesses are mitigated to reduce risks to an acceptable level.

5.5 Information Verification

A formalized POA&M process ensures that steps are taken to verify information. An organization with a mature process will include steps to validate that completed weaknesses have been tested to ensure their mitigation, as well as to ensure the accuracy of all reported information.

5.6 Post Remediation Improvement Efforts

To formalize the POA&M process fully, organizations should be able to apply the knowledge gained from the remediation of weaknesses to future improvement efforts. Over time, information collected from actual POA&Ms, and from the process in general, can be used to advance weakness mitigation effectiveness.

6. Conclusion

The benefits of the POA&M are significant and far-reaching, internally and externally to HHS and each OPDIV. For each OPDIV, the POA&M becomes a comprehensive reference to be used in ongoing efforts to address programmatic and system-specific vulnerabilities. For the Department, the POA&M is an essential management tool for the oversight and mitigation of security weaknesses.

To function as an effective tool, the POA&M must be continually and diligently updated. The operating environment, levels of acceptable risk, and the availability of resources are a small sampling of the many changes that occur on a frequent basis. An effective and successful POA&M document captures each one of these changes in the most concise and complete fashion.

A mature POA&M program requires that the knowledge and efforts of HHS and each OPDIV are sustainable over time and independent of any one person or personnel function. As a central repository, the POA&M eliminates the reliance on one resource and secures institutional knowledge. Although a time-intensive effort initially, the POA&M, if properly maintained, has the potential to be a valuable tool for management and will improve the overall IT security posture of the Department.

Appendix A: Document Feedback

This form is for reviewer suggested corrections, revisions, or updates and is intended to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the U.S. Department of Health and Human Services (HHS), Office of Information Resources Management (OIRM).

By E-mail: SecureOne.HHS@hhs.gov
Subject Line: Guidance Feedback
By Phone: OIRM: (202) 690-6162

Document Title:
>
Section Number:
>
Category of Comment:

A	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
S	Substantive. Substantive comments are provided because sections in the publication appear to be or are potentially incorrect, incomplete, misleading, or confusing.
C	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
M	Major. Major comments are significant concerns that may result in a non-concurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.

Category	**Comment**

Name of Submitting Operating Division (OPDIV):
>
Your Name and Title:
>
Telephone:
>
E-mail:
>
Note: Use an additional blank sheet if needed.

Appendix B: References

Federal Information Processing Standards Publications (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

NIST DRAFT SP 800-30 Rev A, *Risk Management Guide for Information Technology Systems*, January 2004.

Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission and Execution of the Budget,* (Revised July 25, 2003).

OMB Circular A-130, *Management of Federal Information Resources,* November 28, 2000.

OMB Memorandum (M)-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

OMB M-02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plan of Actions and Milestones,* July 2, 2002.

OMB M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 6, 2003.

Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996,* August 21, 1996.

Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002 Title III, of this Act is the Federal Information Security Management Act of 2002 (FISMA)*, December 17, 2002.

Appendix C: Acronyms

C&A	Certification and Accreditation
CAI	Corrective Action Impact
CFO	Chief Financial Officer
CIO	Chief Information Officer
CSO	Chief Security Officer
DOJ	Department of Justice
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act of 2000
GSS	General Support System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IG	Inspector General
INFOSEC	Information Security
IPSO	Information Processing Service Organization
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPDIV	Operating Division
PIA	Privacy Impact Assessment
PMA	President's Management Agenda
POA&M	Plan of Action and Milestones
POC	Point of Contact
SDLC	System Development Life Cycle
SP	Special Publication
USC	United States Code

Appendix D: Glossary

Acceptable Risk—a concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls. (Defined in Draft National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Annex B)

Adequate Security—security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the Operating Division (OPDIV) operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. (Defined in Office of Management and Budget (OMB) Circular A-130, Appendix III, (A)(2)(a))

Availability—ensuring timely and reliable access to and use of information. (Defined in 44 US Code (USC), § 3542)

Confidentiality—(1) assurance that information is not disclosed to unauthorized persons, processes, or devices. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in 44 U.S.C., §3542)

Data Integrity—the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (Defined in NIST SP 800-27, Appendix B)

Department-wide Information Security Program—HHS is required to develop and implement an information security program for the entire Department, including all Operating Divisions. This program must provide information security for the operations and assets of the Department, including operations and assets provided or managed by another Department. (Defined in the Government Information Security Reform Act of 2000 (GISRA), Section 3534 (b)(1))

General Support System (GSS)—an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data-processing center including its operating system and utilities, a tactical radio network, or a shared information-processing service organization (IPSO). (Defined in OMB Circular A-130, (A)(2)(c))

Information—any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, 6(a))

Information Owner—is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that

responsibility even when the data/information are shared with other organizations. (Defined in NIST SP 800-26, Appendix C)

Information Security (INFOSEC)—protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability [Defined in 44 U.S.C., § 3542].

Information Technology—any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by an OPDIV whether the OPDIV uses the equipment directly or it is used by a contractor under a contract with the OPDIV which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources [40 U.S.C., § 1401]. It does not include any equipment that is acquired by a federal contractor incidental to a federal contract. (Defined in the Clinger Cohen Act of 1996, §§5002, 5141 & 5142)

Integrity—(1) the degree to which a system (or system component) prevents unauthorized access to, or modification of, computer programs or data. (Defined in DOJ, SDLC Guidance Document, Appendix A) (2) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (Defined in 44 U.S.C., § 3542).

IT Security Costs—In determining information and IT security costs, federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the agency Inspector General. This includes the costs of:

    - risk assessment
    - security planning and policy
    - certification and accreditation
    - specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
    - authentication or cryptographic applications
    - education, awareness, and training
    - system reviews/evaluations (including security control testing and evaluation)
    - oversight or compliance inspections
    - development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment

- contingency planning and testing
- physical and environmental controls for hardware and software
- auditing and monitoring
- computer security investigations and forensics
- reviews, inspections, audits, and other evaluations performed on contractor facilities and operations.

2. Other than those costs included above, security costs must also include the products, procedures, and personnel (federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

3. Many agencies operate networks, which provide some or all the necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid 'double-counting' agencies should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded; therefore, if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the budget materials. (Defined in FY05 OMB Circular A-11, section 53)

Major Application (MA)—an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST SP 800-18)

Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d))

Major Information System—a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs,

finances, property, or other resources. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should also be evaluated against these criteria. Your agency Capital Planning and Investment Control Process may also define a "major system or project". All major systems or projects must be reported on exhibit 53. In addition, a "major" IT system is one reported on your "Capital Asset Plan and Business Case," exhibit 300. For the financial management mission area, "major" is any system that costs more than $500,000. Additionally, if the project or initiative directly supports the President's Management Agenda Items, then the project meets the criteria of "high executive visibility". Projects that are E-government in nature or use e-business technologies must be identified as major projects regardless of the costs. If you are unsure about what systems to consider as "major", consult your agency budget officer or OMB representative. Systems not considered "major" are "small/other". (Defined in OMB Circular A-11, section 300)

Management Controls—techniques and concerns, normally addressed by an organization's management, that focus on the management of security and risk of an IT system. More expressly, actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions. (Defined in NIST SP 800-16, Appendix C)

Material Weakness—or *significant weakness* is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management. (Defined in NIST SP 800-26, Appendix C)

Operational Controls—procedures and operational methods focusing on mechanisms implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. (Defined in NIST SP 800-18, Appendix D)

Plan of Action and Milestone (POA&M)—(a corrective action plan) a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.
The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (Defined in OMB Memorandum (M) 02-01)

Policy—a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance. (Defined in NIST SP 800-26, Appendix C)

Program—consists of organized activity that contains any number of basic elements such as conducting risk assessments; conducting IT Security training; establishing an incident response capability; writing, establishing, and enforcing policies and procedures; and processes for planning, implementing, evaluating, and implementing remedial action for addressing weaknesses. (Defined in Title III of the E-Government Act)

Program Official—a division director or equivalent who is responsible for a major program or functional area.

Program Review—a program review, in the context of the work required under the Government Information Security Reform Act, is a review of the security status of an operational program and is not a security program itself. Each program must be reviewed annually to ensure: 1) risk assessments occur; 2) policies and procedures are risk-based and cost-effective and comply with existing laws and OMB policy; 3) security awareness training for all employees; 4) management testing and evaluation of the effectiveness of information security policies and procedures; 5) a process for remedial action; and 6) procedures for detecting, reporting, and responding to security incidents. (Defined in OMB guidance and the GISRA, Section 3534 (b)(2)(A-F))

Risk—the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. (Defined in NIST SP 800-30, Appendix E)

Risk Assessment—the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. (Defined in NIST SP 800-30, Appendix E)

Risk Management—the total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. (Defined in NIST SP 800-30, Appendix E)

Security—technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Also referred to IT Security. (Defined in NIST SP 800-16, Appendix C)

Security Controls—the management, operational, and technical controls (i.e., safeguards or countermeasures), prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the

confidentiality, integrity, and availability of the system and its information. (Defined in Draft NIST SP 800-37, Annex B)

Security Program—a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. (Defined in NIST SP 800-16, Appendix C)

Sensitive Data—information whose loss, misuse, unauthorized access to, modification, or destruction, could adversely affect the national interest or the conduct of federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. Sensitive data can relate to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for public release. (Defined in FIPS PUB 102, Appendix A)

Sensitivity— the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components. (Defined in NIST SP 800-16, Appendix C)

System—a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected. (Defined in NIST SP 800-16, Appendix C)

(2) The interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Technical Controls—automated, technological security mechanisms the IT system executes. The controls can provide automated protection for unauthorized access or misuse and facilitate detection of security violations. (Defined in NIST SP 800-18, Appendix D)

Vulnerability—a flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (Defined in NIST SP 800-47, Appendix D)

Appendix E: Weakness Prioritization Methodology

The weakness prioritization methodology focuses on two essential criteria:

- system categorization
- system weaknesses risk level.

Once the system and its weaknesses are categorized and ranked, the Plan of Action and Milestones (POA&M) author will be able to prioritize the weaknesses for mitigation. The following steps outline the process of weakness prioritization.

1. Step 1 – System Categorization

System categorization should be determined in the system's risk assessment according to the criteria articulated in the Federal Information Processing Standards (FIPS) Publication 199, *Security Categorization of Federal Information and Information Systems*. According to FIPS 199, system categorization should be classified as high, moderate, or low, according to the confidentiality, integrity, and availability criteria. The following sub-steps provide the criteria to categorize the system, as well as the system's information.

Step A: Identify Information Types:

First, determine what different types of information the system processes. Table 1 provides several examples of different types of information.

Types of Information	Description
Public	Data that can be directly accessed by the public or requested through the Freedom of Information Act (FOIA) office.
Private	Data that can be directly linked to an individual (Name, Social Security Number, Date of Birth, Driver License Number, Financial Account Information, etc.).
Financial	Data on the financial status of an individual or asset.
Administrative	Data that tracks medical device development.
Identification	Data used to authenticate an asset or individual to a system.

Table 1. Examples of Information Types

Step B: Information Categorization

Once the system's information types have been identified, each must be classified as high, moderate, or low, according to the confidentiality, integrity, and availability criteria outlined in table 2. Figure 1 depicts the calculation for categorizing information based on the impact (i.e., high, moderate, or low) for each security objective (i.e., confidentiality, integrity, availability).

System Categorization (SC) *information type* = ([confidentiality, *impact*], [integrity, *impact*], [availability, *impact*])

Figure 1. System Categorization Formula

Table 2. Potential Impact Definitions for Security Objectives[2]

Security Objective	Level of Impact		
	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on agency operations, (including mission, functions, image, or reputation), agency assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Table 3 illustrates the identified and categorized information types for the system.

[2] Definitions of the categories and rating are defined by the NIST FIBS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Table 3. Examples of Categorized Information Types

Information Type	Confidentiality	Integrity	Availability
SC Public =	*Low*	*Moderate*	*Moderate*
SC Financial =	*High*	*Moderate*	*Moderate*
SC Administrative =	*Low*	*Moderate*	*Low*

Step C: System Categorization

System categorization is the aggregate of information categorization. The highest level of impact of confidentiality, integrity, and availability for each information category indicates the system category. Use the following formula outlined in table 4.

Table 4. System Categorization Calculation

Information Type	Confidentiality	Integrity	Availability
SC Information Category 1 =	*Impact*	*Impact*	*Impact*
SC Information Category 2 =	*Impact*	*Impact*	*Impact*
SC Information Category 3 =	*Impact*	*Impact*	*Impact*
SC System Category =	*Highest Impact level for Confidentiality*	*Highest Impact level for Integrity*	*Highest Impact level for Availability*

The system security category has been calculated in table 5.

Table 5. Example of system Categorization

Information Type	Confidentiality	Integrity	Availability
SC Public =	*Low*	*Moderate*	*Moderate*
SC Financial =	*High*	*Moderate*	*Moderate*
SC Administrative =	*Low*	*Moderate*	*Low*
SC System Category =	*High*	*Moderate*	*Moderate*

2. Step 2 – System Weakness Risk Level

System weakness risk levels should be determined in the system's risk assessment according to the criteria articulated in the Draft National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision A, *Risk Management Guide for Information Technology Systems*, January 2004. During the risk assessment process, weaknesses may be identified and risk ratings should be assigned to the vulnerability to signify the level of impact the vulnerability may have if exploited. The risk level determination process encompasses the following sub-steps:

- Step A–Determine the likelihood of the identified system threat exploiting a specific identified vulnerability.
- Step B–Determine the impact to a system's operation and information should a threat exploit the specific identified vulnerability.
- Step C–Determine the overall risk for the specific identified vulnerability.

The equation shown in figure 2 summarizes how risk is determined for each weakness:

Figure 2. Risk Score

2.1 Step A–Determine the Likelihood

Likelihood is determined by analyzing the intersection of threats and vulnerabilities. The likelihood that a vulnerability will be exploited by a threat will be assessed and described as high, medium, or low. Factors that govern the likelihood of threat exploitation include threat capability, frequency of threat occurrence, and effectiveness of current countermeasures. The descriptions shown in table 6 are used to determine the likelihood level for a threat/vulnerability pair.

Table 6. Likelihood Levels

Likelihood Levels	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

2.2 Step B–Determine the Impact

Impact refers to the magnitude of potential harm that may be caused by threat exploitation. Impact is determined by the value of the resource at risk, both in terms of its inherent (replacement) value and its importance (criticality) to the Department's mission. The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. Table 7 provides a description for each level of impact.

Table 7. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Medium	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

2.3 Step 3–Determine the Risk

After evaluating likelihood and impact, the assessment team will use a risk level matrix with the ratings of high, medium, and low to determine the degree or level of risk to which a system, facility, or procedure might be exposed if a vulnerability is exploited. The level of risk equals the intersection of the likelihood and impact values. For example, based on figure 3, if the likelihood level is 'high' and the impact level is 'low' for a threat/vulnerability pair, then the risk level would be 'medium.'

	Impact		
Threat Likelihood	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Figure 3. Risk Level Matrix

The completion of steps 1 and 2 will assist the POA&M author with prioritization of weaknesses by using the methodologies described in step 3.

3. Step 3 – Weakness Prioritization Process

The following sections outline two example methodologies to use in order to prioritize system weaknesses:

- basic prioritization
- compound prioritization.

3.1 Basic Prioritization Methodology

Formal calculation procedures are useful in demonstrating the implementation of prioritization criteria. The criteria chosen for prioritization, and resulting decisions from implementing prioritization, should be justified appropriately. The basic prioritization methodology assigns weights to a set of criteria: system categorization and weakness risk level. The POA&M author can quantitatively prioritize weaknesses based this criteria. Table 8 displays the basic prioritization methodology assigned weights.

Table 8. Criteria Weights

Weakness Risk Level		System Categorization	
Risk Level	Risk Ranking	Impact Level	Impact Ranking
High	3	High	3
Medium	2	Moderate	2
Low	1	Low	1

The next step after assigning weights to the set of criteria is to multiply the weakness risk level by the system categorization. The outcome is the total weight of the weakness. The total weight can then be used as a prioritization criterion. Table 9 illustrates the basic prioritization methodology calculation of each weakness.

Table 9. Illustrative Basic Prioritization Methodology

Weakness ID	System Categorization			Impact Level Total (D)	Weakness Risk Level (E)	Total Weight (D x E)
	System Impact Level (A) Confidentiality	System Impact Level (B) Integrity	System Impact Level (C) Availability			
	(A + B + C)=D					
SYSY_2004_B_1	3	3	3	9	2	18
ABC 1	3	2	3	8	3	24
ABC 2	3	1	3	7	2	14
SYSY_2004_B_2	2	1	3	6	1	6
SYSX_2004_A_2	1	2	1	4	2	8
SYSX_2004_A_1	3	2	1	5	1	5

Once the total weight of a weakness is identified, then the weaknesses can be prioritized for mitigation. Table 10 shows the ranking order of the weaknesses.

Table 10. Weakness Final Prioritization

Weakness ID	Total Weight (D x E)	Ranking Order of Weakness Mitigation
SYSY_2004_B_1	18	2
ABC 1	24	1
ABC 2	14	3
SYSY_2004_B_2	6	5
SYSX_2004_A_2	8	4
SYSX_2004_A_1	5	6

It is recommended that before implementing corrective actions to mitigate the weaknesses, the organization's management should approve the ranking order listing of the weaknesses. Management may have specific weaknesses that need to be addressed for reasons that are not captured in purely quantitative risk prioritization construct (e.g., long-outstanding weaknesses, weaknesses with other dependencies).

3.2 Compound Prioritization Methodology

The following methodology is based on some of the components of the forthcoming NIST SP 800-65, *Integrating IT Security Into the Capital Planning and Investment Control Process* guidance document. This methodology addresses systems and weaknesses by system categorization, weakness risk levels, compliance with NIST SP 800-26, the agency's missions and goals, and total corrective action cost to mitigate

all weaknesses. The compound prioritization methodology inputs are highlighted in table 11 and detailed in the following subsections.

Table 11. Compound Prioritization Methodology Inputs

Column	Heading	Content—How to Complete
1	System Name	The unique identifier for the system.
2	System Categorization	The level of impact to confidentiality, integrity, and availability pertaining to information and systems.
3	IT Security Controls Compliance Gap %	The system's percentage of non-compliance with the selected IT security controls.
4	Corrective Action Cost	The total cost to remediate the identified weaknesses.
5	Corrective Action Impact (CAI)	The CAI shows which investment presents the most value to the agency's identified priorities from the funds available.
6	Ranking per Corrective Action Impact	The overall ranking level (high, medium, or low) of the CAI score based off the stakeholder CAI range.

3.2.1 System Name

The system name should be a unique identifier for the system. It is recommended to use the same system name identifier reported in the POA&M.

3.2.3 IT Security Controls Compliance Gap Percentage

Compliance with established IT security controls is a primary input to the prioritization process. IT security controls compliance is a broad term that can incorporate several different types of security compliance. It is up to Departmental management and IT security stakeholders to determine which IT security controls are essential inputs for their POA&M process. The inputs will depend upon the unique business and IT security requirements of the organization. For example, the following inputs could be used individually or collectively to measure IT security controls compliance:

- percent compliance with NIST SP 800-26, *Security Self Assessment Guide for Information Technology Systems* topic areas
- percent compliance with Certification and Accreditation (C&A) criteria
- percent compliance with IT privacy controls.

For the compound prioritization methodology, IT security control compliance will be based on NIST SP 800-26. The security compliance gap is the system's percentage of non-compliance with the IT security controls in NIST SP 800-26. For example, if a system is 40 percent compliant with the 17 NIST SP 800-26 topic areas, then the security compliance gap is 60 percent (100 percent compliance minus the existing 40 percent compliance).

3.2.4 Corrective Action Cost

The corrective action cost is the total cost to mitigate all the identified weaknesses from the POA&M. This total cost is derived either from historical prices or by using an organizational-specific costing tool.

3.2.5 Corrective Action Impact

The corrective action impact (CAI) calculation presents the most value to the agency's identified priorities from the funds available. Dividing the security compliance gap percentage by the cost of the corrective action will calculate the CAI. From this calculation, a ratio of security vulnerability to corrective action cost is obtained. The resulting ratio provides a proportion of results to cost. The higher the impact proportion, the greater the effect of corrective action. Figure 4 illustrates the calculation for the corrective action impact; note that the results are multiplied by the value 100,000 to facilitate further calculations.

$$\left(\frac{\text{Corrective Action Security Compliance Gap\%}}{\text{Corrective Action Cost}} \right) X \ 100{,}000$$

Figure 4. Corrective Action Impact Formula

3.2.6 Ranking per Corrective Action Impact

The ranking per CAI is the overall ranking level according to high, medium, and low of the CAI score based off the stakeholder's CAI range. This example shows that the stakeholders have determined that CAIs greater than 1.0 are 'High', CAIs between .99 and .50 are 'Medium', and those .49 and below are 'Low'. Table 12 can be used as a reference for these scores. Before implementing corrective actions, IT security management should have oversight authority on the prioritized list of systems to further ensure that the organization's concerns are met.

Table 12. Rating Corrective Action Impact Scores

Ranking CAIs	
CAI Range	**Value to Agency**
1.0 < CAI	High
.99 ≥ CAI ≥ .50	Medium
.49 ≤ CAI	Low

Table 13 illustrates the compound prioritization methodology for seven fictitious systems.

Table 13. Example Compound Prioritization Inputs

System Name	System Categorization			Impact Level Total (D)	IT Security Controls Compliance Gap %	Corrective Action Cost	Corrective Action Impact (CAI)	Ranking per Corrective Action Impact
	System Impact Level (A) Confiden-tiality	System Impact Level (B) Integrity	System Impact Level (C) Avail-ability					
	(A + B + C)=D							
X	3	3	3	9	60%	$17,680	3.39	High
Y	3	2	3	8	40%	$61,520	.65	Medium
Z	3	1	3	7	70%	$110,000	.63	Medium
U	2	1	3	6	25%	$75,500	.33	Low
V	1	2	1	4	80%	$250,000	.32	Low
W	2	2	1	5	20%	$395,000	.05	Low
T	1	1	3	5	90%	$18,500	4.86	High

The seven fictitious systems can be prioritized based on the CAI percentage and the impact level ranking. This is accomplished by first putting the systems in order of high to low according to the CAI percentages, and then in order from highest number to lowest number according to the impact level. Table 14 displays the systems prioritized.

Table 14. System Prioritization

Prioritization Order	System Name	Impact Level Total (D)	Ranking per Corrective Action Impact
1	X	9	High
2	T	5	High
3	Y	8	Medium
4	Z	7	Medium
5	U	6	Low
6	W	5	Low
7	V	4	Low

Once systems are prioritized according to CAI and impact levels, the weaknesses within the systems need to be prioritized to help ensure that security dollars are applied towards the most pressing weaknesses. For example, System X in table 14 ranked as the highest priority system; however, the weaknesses within System X still need to be prioritized for effective IT security spending. Section 3.2.7 outlines the process of ranking weakness for each system.

3.2.7 System Weaknesses Prioritization

The weaknesses within the systems also need to be prioritized. Since System X is the highest priority system, its weaknesses should be prioritized first. To rank order the weaknesses within System X's POA&M, the stakeholder's rankings of the IT security controls are necessary. Table 15 illustrates an example with fictitious organization's rankings of IT security controls following a facilitated rank ordering session with an analytical hierarchy tool.

If stakeholders ranked IT privacy as the most pressing IT security activity, then all weaknesses in System X's POA&M associated with privacy issues would take precedence. Following this prioritization strategy within each system's POA&M, project managers can help ensure they are using security funds to address weaknesses that are important to overall organization's IT security initiatives.

Table 15. IT Security Control Rankings

NIST SP 800-26 Topic Areas	
Ranking	**IT Security Control**
1	Identification and Authentication
2	Contingency Planning
3	Logical Access Controls
4	Audit Trails
5	Risk Management
6	System Security Plan
7	Incident Response Capability
8	Authorize Processing
9	Hardware and Systems Software Maintenance
10	Review of Security Controls
11	Security Awareness, Training, and Education
12	Physical Security
13	Data Integrity
14	Personnel Security
15	Production, Input/Output Controls
16	Life Cycle
17	Documentation

Table 16 displays System X's POA&M, with an illustrative column that indicates the related IT security control area for each specific weakness.

Table 16. System X POA&M

1	2	3	4	5	6	7	8	9	10	11	12
Weakness Identifier	Weaknesses	IT Security Control Mapping	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status	Comments	Risk Level
X_2003_C_1	1—Hiring, transfer and termination procedures are not established	Personnel Security	Center ISSO	$7,680	1/30/04	Develop hiring, transfer, and termination procedures 1/15/04		NIST self assessment 10/15/03	Completed 12/31/03		Low
						Distribute procedures 1/30/04					
X_2003_A_2	2—Contingency plan not tested	Contingency Planning	System X ISSO	$10,000	2/15/04	Schedule and conduct contingency plan test 2/15/04		NIST self assessment 10/15/03	Ongoing		Medium

Based on the stakeholder's rankings, weakness X_2003_A_2 would receive priority over weakness X_2003_A_1 because contingency planning received a ranking of two in table 14 while personnel security received a ranking of 14. After completing the prioritization of weaknesses in System X's POA&M, efforts would shift to System T's POA&M, per the prioritization in table 14. Following this prioritization strategy within each system's POA&M, project managers can help ensure they are using security funds to address weaknesses that are important to overall IT security stakeholders.

Again, as with the prioritized list of systems, management should have oversight authority on the prioritized list of weaknesses within each prioritized system's POA&M to help ensure that overall IT security goals are met.

By following this prioritization methodology, POA&M weaknesses can be prioritized according to system risk level, the impact the corrective action will have, and stakeholder priorities. With additional management oversight throughout the process, weaknesses can be effectively prioritized in alignment with the Department's priorities and IT security concerns.

Appendix F: POA&M Sample Submission

Sample Agency or Program-level Plan of Action and Milestones

Agency, Component, and Program Name—Department of Good Works, Major Service Administration

1	2	3	4	5	6	7	8	9	10	11
Weakness Identifier	Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status	Comments	Risk Level
SYSX_2004_C_1	1—No program-level security program/plan	Program office and agency CIO	200 hours, current staff	12/31/03	Draft plan prepared and circulated for user input—7/31/03		IG FISMA Report, 9/02	Completed 12/31/03		
					Comments reviewed, final draft to Administrator for approval and publication—12/31/03					
SYSX_2004_C_2	2—No program to report external security incidents to law enforcement and GSA	Program office and agency CIO	$20,000, current funding	8/31/04	Consult with agency IG, FBI/NIPC, and GSA—12/31/03		IG FISMA Report, 9/03	Ongoing		
					Draft plan and procedures—3/31/04					
					Finalize and disseminate plan—5/31/04					
					Train staff and implement—8/31/04					

Weakness description.

Office or Org, not a person's name.

Indicate if resources are from current, new, or reallocated sources.

Field cannot be changed once submitted.

When a corrective action is not completed as originally scheduled, indicate new date.

Include expected completion date with each milestone.

Include date weakness was first identified.

Completed means weakness has been fully resolved and tested.

Add additional detail or clarifications for any previous entries.

This column is to record the level of risk that the weakness may be exploited.

System-level Plan of Action and Milestones

System Name	System Criticality as defined by FIPS	Confidentiality	Availability	Integrity	If no weakness, provide a reason
Generic	Medium	Medium	Medium	Medium	

Exhibit 300	Project ID (300)	Project Name	Exhibit 53	Project ID (53)	Security Costs	Accreditation Date (Actual or Scheduled)
Yes	009-22334-55873	Infrastructure				8/31/04

1	2	3	4	5	6	7	8	9	10	11
Weakness Identifier	Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status	Comments	Risk Level
SYSX_2004_C_1	Standard procedures for disposition and sharing of data not established.	System Owner, System ISSO, Center ISSO	100 hours, current staff	10/31/03	Draft standard procedures for disposition and sharing of data—7/31/03		Risk Assessment 4/30/03	Completed 10/31/03		Medium
					Finalize standard procedures for disposition and sharing of data—10/31/03					
SYSX_2004_C_2	System application documentation is not maintained at an off-site storage location, and the backup site is not geographically removed from the primary site(s).	IT Director, Center ISSO	$20,000, current funding	3/1/04	Evaluate and identify appropriate off-site location—1/31/04		NIST Self-Assessment 11/31/03	Delayed		Medium
					Maintain system application documentation off-site and move backup site to a geographically removed location—3/1/04	5/31/04			Site needs further preparation before move can be accomplished	
SYSX_2004_C_3	System security plan not updated	OPDIV ISSO Center ISSOs	75 hours, current staff	7/31/04	Identify changes that have occurred on system—4/30/04		IG Audit, 3/04	Ongoing		Medium
					Draft updated system security plan—6/30/04					
					Finalize updated system security plan—7/31/04					

Office or Org, not a person's name.

Field cannot be changed once submitted.

Once completed, include date of actual completion.

This column is to record the level of risk that the weakness may be exploited.

Indicate if resources are from current, new, or reallocated services.

Include expected completion date with each milestone.

Include date weakness was first identified.

Indicate weakness status as delayed if not resolved by scheduled completion date.

Weakness description.

When a corrective action is not completed as originally scheduled, indicate new date.

Reasons or explanations should be offered for any weakness that shows "delayed".